Kaspersky Security for Internet Gateway

境界最前線における保護

カスペルスキー製品は 2018 年第 2 四半期だけで、187 の国と地域のインターネットリソースから仕掛けられた 9 億 6,000 万以上の攻撃をブロックしました。企業がインターネットにいかに大きく依存しているかを考えれば、このような攻撃の多さも不思議ではありません。しかし、企業がインターネットなしに存続できないのならば、そのセキュリティを無視して存続することもまた不可能です。

エンドポイントは主たる攻撃対象であり、Web リソースがユーザーによって利用される場所、そして攻撃者がソーシャルエンジニアリングを巧みに利用して人の行動に影響を与ぼすことが可能な場所です。一方、ユーザーによる人的要因は予想が難しく、一旦エンドポイントが侵害されると被害拡大の防止や解決のためのコストも膨大なものになります。感染がエンドポイントに達する前に対処することが、かつてないほど重要になっているのです。

特長

- リアルタイムの次世代型アンチマルウェア / アンチフィッシングによる保護
- ランサムウェアが企業ネットワーク内に入り込む前にブロック
- 誤検知数を増やすことなく、検知率を大幅に向上
- コンテンツフィルタリングによって重要なファイルの送信をブロックしてデータ漏洩を防止
- Web リソースの利用を統制するウェブコントロール
- SSL で暗号化されたトラフィック監視によるセキュリティ強化
- 高負荷のネットワークに合わせてスケーリング可能
- ゼロアワーの脅威からの保護
- Kaspersky Security Network のグローバルな脅威インテリジェンスによる支援
- MSP や多角的ビジネスのためのマルチテナント機能

Kaspersky Security for Internet Gateway は、ゲートウェイレベルでの外部からの脅威を 95% 阻止してエンドポイントへの到達を防ぐことで、それらの脅威がユーザーやワークステーションに及ぼす影響を大幅に抑えます。既存の保護インフラストラクチャに Kaspersky Security for Internet Gateway を加えれば、侵害のリスクを減らして事業継続性を確保することができます。

機能と利点

外部からのマルウェアやランサムウェアのブロック

Kaspersky Security for Internet Gateway は、多重の検知層とそれらを支える機械学習技術によって、高度なマルウェアやランサムウェアであっても、IT インフラストラクチャへの侵入やビジネスクリティカルなプロセスの中断を防ぎます。Kaspersky Lab のエンジンの性能は、独立機関によるテストで最高評価を獲得することで常に実証されています。

フィッシングの無効化

フィッシングでは、ユーザーに対して詐欺用のリソースを正規のものに見せかけたサイトが利用されます。この手口に引っかかった場合、個人情報のほか金融情報までも失う可能性があります。カスペルスキーの高度なクラウド支援型アンチフィッシングシステムは、悪意のあるフィッシング URL について世界中から収集したデータを利用して、ダウンロードされたファイルに含まれる既知、未知、ゼロアワーのフィッシング URL から保護します。

情報漏洩の阻止

効果的なコンテンツフィルタリング機能によって、管理者が設定する各種パラメータに基づいてネットワーク内を移動するすべてのコンテンツにフィルタをかけられるため、感染被害はもちろん、データ漏洩のリスクを抑えることができます。

インターネット利用の統制によるリスク削減と生産性向上

管理者が、ウェブコントロールのシナリオについてのカスタムルールを設定、作成して、特定の Web リソースタイプの利用を制限することができます。これにより、マルウェアサイトとしても機能しそうな Web リソースからの感染リスクを軽減し、また不必要なオンライン活動をなくすことで生産性を向上させることができます。

HuMachine™ を利用した、脅威からの多層型保護

カスペルスキーの次世代型マルウェア保護には、複数のプロアクティブなセキュリティ層が組み込まれています。これには、機械学習アルゴリズムに基づく層や、強力なクラウドベースメカニズムが支える層が含まれます。

Kaspersky Security Network と連携することで、最新の脅威が迅速かつ正確に検知されます。アップデートを待つ必要もなく、待つ間に危険にさらされることもありません。

- **グローバルな脅威インテリジェンス：**Kaspersky Security for Internet Gateway は脅威の情勢が変化する中、世界中から収集された最新のデータを利用します。
- **機械学習：**グローバルな脅威インテリジェンスのビッグデータは、機械学習アルゴリズムと人間の専門知識を結集して処理されます。これにより、実績ある高い検知率と極めて低い誤検知率を実現しています。

トラフィック監視の強化

製品のアーキテクチャにより、SSLで暗号化された企業内トラフィック監視を簡単に導入できます（このような監視は「SSL Bump」または「corporate man-in-the-middle」とも呼ばれます）。SSL で暗号化された Web トラフィックがインターネット通信のデファクトスタンダードになっていることから、このトラフィック監視は極めて重要な機能です。

ビジネスの規模に合わせたスケーリング

Kaspersky Security for Internet Gateway は、高負荷のシステムに合わせて完全にスケーリング可能であり、複数ノードの管理と階層型デプロイを容易に実行できます。

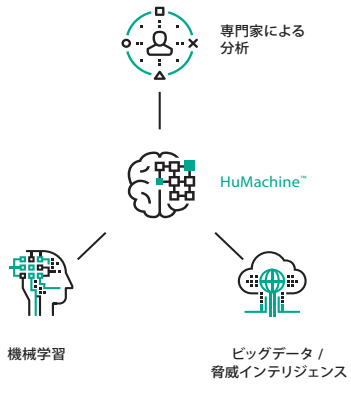
柔軟な管理と完全な可視化によって Web ベースの脅威への対処が容易に

Kaspersky Security for Internet Gateway の大きな特徴は、柔軟かつ使いやすい管理システムです。

- 刷新された Web コンソールを使って、セキュリティ管理者が完全な可視化と柔軟な管理を行うことができます。
- 利便性に優れたダッシュボードから、イベントなどのゲートウェイのセキュリティ状況をすばやく効果的に概観できます。
- 管理者が柔軟なルール設定システムを利用して効果的な保護シナリオを設定し、ゲートウェイのセキュリティをより細かく管理できます。
- ロールベースのアクセス制御を行うことで、管理上のエラーのリスクを最小限に抑えます。これは特に、複数のセキュリティ管理者がいて、それぞれに異なるレベルの責任が割り当てられるような大企業や、サービス提供先のテナントが複数いる MSP にとって便利な機能です。
- Active Directory との統合によって、既存のユーザーやグループの情報に基づいて、Web の利用に関するルールを作成できます。
- 既存のセキュリティ情報 / イベント管理（SIEM）システムと統合し、ゲートウェイレベルのイベントを取得することで、企業のセキュリティの状況がさらに把握しやすくなります。

マルチテナントのサポート

Kaspersky Security for Internet Gateway は、マルチテナント管理機能と柔軟なライセンス管理機能をサポートしており、適度な管理権限をテナントの管理者に委譲することができます。MSP や多角的ビジネスに最適な機能です。



株式会社カスペルスキー

サイバー脅威に関する最新情報：　www.securelist.com
IT セキュリティに関する最新情報：　blog.kaspersky.co.jp
ご購入相談窓口：　jp-sales@kaspersky.com

www.kaspersky.co.jp

PMM-1035-201811